

STATE OF ALABAMA

Information Technology Standard

Standard 640-04S1: VoIP Security

1. INTRODUCTION:

Voice over Internet Protocol (VoIP) technology allows traditional data and voice communications to be transmitted together over State of Alabama Ethernet-based networks as well as the Internet via the TCP/IP protocol.

2. OBJECTIVE:

Provide the minimum requirements for the design, deployment, and security management of VoIP technology.

3. SCOPE:

The following requirements apply to all State of Alabama organizations that plan, manage, or utilize VoIP technology.

4. REQUIREMENTS:

The following requirements, based the recommendations of the National Institute of Standards and Technology (NIST) found in Special Publication 800-58: Security Considerations for Voice Over IP Systems, shall be applied to all VoIP deployments with specific concentration on Sensitive or Confidential data and voice transmissions utilizing VoIP technology on State of Alabama network resources as well as any other public network (i.e., the Internet).

4.1 VoIP SYSTEM STANDARDS

Policy: Develop appropriate network architecture for data and voice considerations; security and technical requirements shall be specified in applicable standards.

Separate voice and data on logically different networks when possible. Using multiple IP subnets for voice and data traffic, with separate DHCP servers for each, allows for easier integration of intrusion detection and VoIP firewall protection.

At the voice gateway disallow H.323, SIP, and other VoIP protocols from the data network. Use strong authentication and access control on the voice gateway system.

A mechanism to allow VoIP traffic through firewalls (such as Application Level Gateways or Session Border Controllers) is required.

When practical to the design, stateful packet filters shall be used to track the state of connections and to deny packets that are not part of a properly originated call.

Use IPSec or Secure Shell (SSH) for all remote management and auditing access. If practical, avoid using remote management at all and do IP PBX access from a physically secure system.

Special consideration must be given to E-911 emergency services communications because in some cases E-911 automatic location service is not available with VoIP.

All VoIP network and server components must be physically secured in accordance with applicable State standards.

VoIP-ready firewalls and other appropriate protection mechanisms shall be employed.

Enable, use, and routinely test the security features that are included in VoIP systems.

VoIP transmissions that contain sensitive and/or confidential content shall be encrypted either by the VoIP endpoints or by other network encryption resources.

VoIP softphone systems shall not be used to convey sensitive or confidential content or when privacy issues are involved.

Where wireless access devices are to be integrated onto the VoIP environment, secure the wireless devices in accordance with State Wireless Client Standard 640-03S2.

4.2 RISK MANAGEMENT

Policy: Ensure the organization has examined and can acceptably manage and mitigate the risks to State of Alabama information, system operations, and continuity of essential operations when deploying VoIP systems.

Vulnerability assessments of the VoIP solution shall be conducted on a semi-annual basis or whenever significant system changes occur.

Specific security controls for the VoIP solution, especially those pertaining to confidentiality and privacy, shall be continuously monitored and reported in accordance with applicable State standards.

Prior to deployment of any VoIP solution by any State of Alabama agency, that agency should advise State legal counsel of the intent to deploy a VoIP solution and seek appropriate legal guidance to ensure compliance with State and Federal Laws that, for example, address privacy issues, call log retention, and potential monitoring of VoIP network traffic.

5. DEFINITIONS:

SOFTPHONE: Systems which implement VoIP using an ordinary PC with a headset and special software.

VOICE OVER INTERNET PROTOCOL (VoIP): Also referred to as IP Telephony, Internet telephony, Broadband telephony, Broadband Phone, and Voice over Broadband, VoIP is the routing of voice conversations over the Internet or through any other IP-based network.

6. ADDITIONAL INFORMATION:

6.1 POLICY

Information Technology Policy 640-04: Voice Over Internet Protocol

6.2 RELATED DOCUMENTS

Information Technology Standard 640-03S2: Wireless Clients

Information Technology Standard 650-01S1: Physical Security

Information Technology Standard 670-02S1: Monitoring and Reporting

Signed by Eugene J. Akers, Ph.D., Assistant Director

7. DOCUMENT HISTORY:

Version	Release Date	Comments
Original	2/16/2007	